V-ONE
Security for a Connected World

Virtual Cryptographic Authentication Token (SmartPass VCAT)

FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

Level 1 Validation

August 3, 1998

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the V-ONE Virtual Cryptographic Authentication Token (SmartPass VCAT). This Cryptographic Module Security Policy is part of the FIPS 140-1[1] documentation prepared by V-ONE for validation of the SmartPass VCAT module. The SmartPass VCAT provides robust security in a flexible software module, meeting all FIPS 140-1 Level 1 requirements. This security policy describes how the SmartPass VCAT meets the FIPS 140-1 requirements, and how the SmartPass VCAT is securely used within V-ONE products.

1.2 Audience

This document in intended for FIPS 140-1 evaluators, National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) reviewers, and customers interested in the SmartPass VCAT's functionality and compliance with FIPS 140-1. This security policy describes the SmartPass VCAT using technical terminology associated with computer security and FIPS 140-1. Readers seeking additional information are referred to the following sources:

> For more detailed information about the SmartPass VCAT and V-ONE's entire product line, please visit the V-ONE web site at http://www.v-one.com.
>
> Fore more information about the FIPS 140-1 standard and validation program please visit the NIST web site at http://csrc.nist.gov/cryptval.
>
> For answers to technical or sales related questions please refer to the contacts listed on the V-ONE web site at http://www.v-one.com.

2 The SmartPass VCAT

The V-ONE Virtual Cryptographic Authentication Token (SmartPass VCAT) is a software cryptographic module which provides key generation, storage, and exchange services. These services are modeled after those provided by popular smartcards, allowing seamless substitution of software or hardware tokens. Whether V-ONE customers require the high-security provided by hardware cryptography, or the lower cost that comes with software-only implementations, the SmartPass VCAT allows all of V-ONE's MaxVPN products the flexibility to support both.

---

[1] Federal Information Processing Standards Publication 140-1 -- *Security Requirements for Cryptographic Modules.* (FIPS 140-1)

2.1 SmartPass VCAT Functionality Overview

The SmartPass VCAT uses DES (Data Encryption Standard, FIPS PUB 46-2) encryption to store keys, data, and files in a single secure file on the hard disk of a personal computer. The module maintains a set of eight DES keys (created with FIPS 171 and ANSI X9.17 Appendix C compliant random number generation and DES key generation). These keys are stored encrypted with up to seven separate user passwords and a single Crypto Officer password referred to as PINs. Each user of the SmartPass VCAT can create encrypted key files suitable for storing cryptographic keys, sensitive data files, session keying information, or session data files. The SmartPass VCAT allows users to specify read, write and update access for each file for other users of the SmartPass VCAT.

The SmartPass VCAT will generate ephemeral session keys by accepting a challenge and generating a response and DES session key. SmartPass VCAT users can then execute encrypted sessions using the session and store temporary session files encrypted with that key.

2.2 Module Interfaces

The SmartPass VCAT is officially considered to be multi-chip standalone module for FIPS 140-1. As such, the module must include a computer running an operating system (OS) and interfacing to the computer keyboard, mouse, screen, floppy drive, CD-ROM drive, speaker, microphone inputs, serial ports, parallel ports, and power plug. However, once information is processed through these physical interfaces, the SmartPass VCAT software module provides a logical interface through an Application Programming Interface (API). This logical interface exposes services through API functions to other programs such as V-ONE's SmartGate and SmartWall.

Thus, there is a single API interface provided by the SmartPass VCAT, which is further logically divided into data input, data output, control input, and status output interfaces. Since it is a software module, the SmartPass VCAT does not provide a separate power or maintenance access interface beyond the power interface provided by the personal computer itself. Data input is represented by input parameters described in functions in the *SmartPass VCAT Software Design Overview Level 1 Validation.* Data output is logically provided through output parameters, control input is provided by the API function calls, and status output is provided by the return codes from each function.

2.3 Roles and Services

The SmartPass VCAT supports two distinct roles using PIN code authentication: Crypto Officer and User. There is a single Crypto Officer role for each SmartPass VCAT with a single Crypto Officer PIN code. Similarly, there is a single User role for the SmartPass VCAT, but there are seven separate User PIN codes. This allows the SmartPass VCAT to support up to seven distinct User identities or groups of Users.

2.3.1 Authentication

Both the users and Crypto Officer authenticate to the SmartPass VCAT by providing a PIN with the CheckCode function. Each User and Crypto Officer PIN code is actually an 8-byte case-insensitive password that may contain alphanumeric, ASCI or binary values.

2.3.2 Services

The SmartPass VCAT offers the following API functions to implement the services that were described in section 0:

CreateNew	**Clear**	**LoadCode**
GetSerialNumber	**GetCurrentFileInfo**	**GetCurrentFileNumber**
LoadReader	**UnloadReader**	**OpenReader**
CloseReader	**CheckCode**	**UpdateCode**
SelectFile	**MakeFile**	**EraseFile**
ReadFile	**WriteFile**	**UpdateFile**
LockFile		
SessionInit	**SessionFinal**	
WriteFileCipher	**UpdateFileCipher**	**ReadFileCipher**

2.3.3 Crypto Officer Role

The role of the Crypto Officer includes creation and destruction of the SmartPass VCAT, and initialization of the SmartPass VCAT including User PINs. The Crypto Officer does this using the *CreateNew* function, which initializes a blank SmartPass VCAT with default PIN codes. The Crypto Officer then uses *LoadCode* to change the default PIN codes to values that will be given to the Users. At any time subsequent to this, the Crypto Officer (and only the Crypto Officer) may run the *Clear* function to destroy the SmartPass VCAT, overwriting the encrypted keys in the SmartPass VCAT file with zeros.

The following are Crypto Officer functions:

CreateNew	**Clear**	**LoadCode**

In addition to the above, the Crypto Officer role is also granted full User role permissions, acting as if she were User 0.

2.3.4 User Role

The SmartPass VCAT User role includes creation, storage and reading or encrypted files on the SmartPass VCAT, as well as symmetric key session functions. The first action of a user is usually to change the PIN code assigned by the Crypto Officer using the *UpdateCode* function. Subsequent to this, a User can exercise the following API functions under the User role:

GetSerialNumber	**GetCurrentFileInfo**	**GetCurrentFileNumber**
LoadReader	**UnloadReader**	**OpenReader**
CloseReader	**CheckCode**	**UpdateCode**

SelectFile	**MakeFile**	**EraseFile**
ReadFile	**WriteFile**	**UpdateFile**
LockFile		
SessionInit	**SessionFinal**	
WriteFileCipher	**UpdateFileCipher**	**ReadFileCipher**

2.4 Finite State Machine

The SmartPass VCAT is designed around a Finite State Machine (FSM) which is detailed in a V-ONE proprietary document (*Virtual Cryptographic Authentication Token (SmartPass VCAT) FIPS 140-1 Proprietary Finite State Machine – Level 1 Validation*). Parties interested in reviewing this document should contact V-ONE through the sources listed in section 0.

2.5 Physical Security

The SmartPass VCAT is a software module and runs on both Windows95 and Windows NT operating systems. However, for FIPS 140-1 purposes, the module was evaluated against Level-1 FIPS 140-1 physical security requirements when running on a standard Intel-compatible personal computer with the Windows95 operating system. This platform meets all Level-1 FIPS 140-1 physical security requirements, providing a multi-chip standalone module with production grade equipment, standard passivation, and a strong enclosure.

2.6 Software Security

The SmartPass VCAT software is written in C and C++ according to the documentation in *Virtual Cryptographic Authentication Token (SmartPass VCAT) Software Design Overview*
Level 1 Validation. This document is proprietary, and parties wishing to review it should contact V-ONE through the sources listed in section 0.

2.7 Operating System Security

The SmartPass VCAT software is implemented as a single loadable module, which is run on Microsoft's Windows 95 or Windows NT platforms. (The evaluated platform for the module is Windows 95.) The module is a single dynamic link library (DLL) and is always distributed as an executable to discourage unauthorized modification. Additionally, a cryptographic mechanism is used within the module to help ensure that the code has not been accidentally or ineptly modified from its evaluated configuration (see section 0).

Since the SmartPass VCAT is implemented as a DLL, the API functions can only be called one at a time to access the SmartPass VCAT file. As depicted in Figure 1, the LLVCAT DLL is loaded into a code segment in memory, with a separate data segment and a pointer to the physical SmartPass VCAT file.

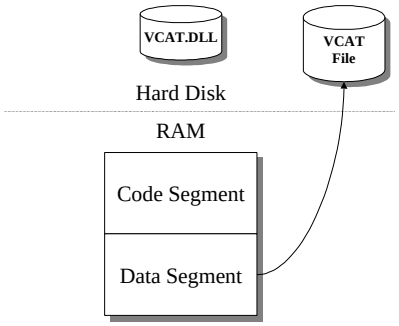

Figure 1 – Loading of LLVCAT.DLL into RAM

The LLVCAT.DLL runs on a the Windows 95 operating system which has been defined for FIPS purposes to be a single-user operating system. A user of the computer may load a second copy of the DLL, as depicted in Figure 2, with a separate data segment. The second SmartPass VCAT module will apply the same access controls to the physical SmartPass VCAT file, maintaining the integrity of the SmartPass VCAT.

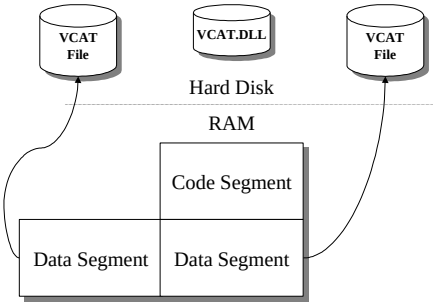

Figure 2 – Single use of an individual SmartPass VCAT file

2.8 Cryptographic Key Management

The SmartPass VCAT uses three classes of cryptographic keys: SmartPass VCAT keys, password-based encryption (PBE) keys and ephemeral session keys. All three types of keys are generated or managed differently as described below.

When a Crypto Officer first creates a SmartPass VCAT, eight User DES keys (SmartPass VCAT keys) are created using the ANSI X9.17 random number generator described in section 0. SmartPass VCAT Users will employ these keys for encryption and decryption of the virtual files within the SmartPass VCAT physical file. Eight copies of these eight keys are then encrypted using PBE keys derived from the Crypto Officer and seven User PINs. These PBE keys are DES keys that are regenerated using the SHA-1 hashing algorithm whenever they are required. The PBE keys are used to encrypt the SmartPass VCAT keys, which are then stored in the PIN code records in the physical SmartPass VCAT file. Users successfully authenticating as described in section 0 can decrypt a set of the module DES keys by providing the correct PIN.

In addition to these types of keys, users can create ephemeral DES session keys using a simple challenge-response protocol. When a SmartPass VCAT user receives a challenge, it can be provided to the SmartPass VCAT, which will initiate a session by creating a

response and generating a session DES key. The response can be transmitted to the creator of the challenge, and the SmartPass VCAT can subsequently use the session key to encrypt files for temporary storage of information. Session keys are ephemeral and are destroyed when the session is terminated.

All permanent keys in the SmartPass VCAT are stored in encrypted form, and are destroyed (overwritten by zeros) when the Crypto Officer issues a clear command to the module.

2.9 Cryptographic Algorithms

The SmartPass VCAT uses DES for encryption of files and stored data, and integrity checks; and uses SHA-1 for message digests in password-based encryption, random number generation, etc. The SmartPass VCAT uses the V-ONE SHA-1 module and the V-ONE DES module.

The V-ONE SHA-1 module implements the Secure Hashing Algorithm (SHA-1), and has been validated as conforming to Federal Information Processing Standard Publication (FIPS PUB) 180-1, *Secure Hash Standard (SHS)*. V-ONE has been issued a certificate signed by the National Institute of Standards and Technology (NIST) and the Canadian Security Establishment (CSE), and is listed on the official validation website (http://csrc.nist.gov/cryptval/dss/dssval.htm).

The V-ONE DES module implements the Data Encryption Standard (DES) and has been validated as conforming to Federal Information Processing Standard Publication 46-2, *Data Encryption Standard (DES)*. The V-ONE DES module was validated by NIST using the Monte Carlo test described in NBS Special Publication 500-20. V-ONE has been issued a certificate signed by the National Institute of Standards and Technology (NIST) and the Canadian Security Establishment (CSE), and is listed on the official validation website (http://csrc.nist.gov/cryptval/des/desval.htm).

The SmartPass VCAT ensures correct operation of both the V-ONE SHA-1 module and V-ONE DES modules using cryptographic algorithm self-tests described in section 0.

2.10 EMI/EMC

Although the SmartPass VCAT consists entirely of software, the FIPS 140-1 evaluated platform is run on a standard PC which has been tested for an meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC Part 15.

2.11 Self Tests

The SmartPass VCAT includes several self-tests to ensure the integrity and correct operation of the module. These include the following:

- SmartPass VCAT Module Software Test

- SHA-1 Cryptographic Algorithm Known Answer Test
- DES Encrypt Cryptographic Algorithm Known Answer Test
- DES Decrypt Cryptographic Algorithm Known Answer Test
- Continuous Random Number Generator Test

2.11.1 SmartPass VCAT Module Software Test

The SmartPass VCAT software module performs a self-integrity check automatically every time it is loaded. The module computes a DES Data Authentication Code (DAC) over the entire module per FIPS PUB 113, and compares the result to a separately stored version of the DAC. Should the SmartPass VCAT module software be corrupt or tampered with, the SmartPass VCAT Module Software Test will fail, alerting the user to the problem and will refuse to load the module.

2.11.2 Known Answer Tests

The SmartPass VCAT software automatically performs known answer tests of all cryptographic algorithms during module startup. This includes SHA-1 hashing a known block and comparing against the stored answer, DES encryption of a known block and comparison against the expected ciphertext, and DES decryption of a known block and comparison against the expected plaintext.

2.11.3 Continuous Random Number Generator Test

The SmartPass VCAT incorporates the V-ONE random number generator (RNG). This RNG is compliant with American National Standards Institute (ANSI) X9.17 Appendix C random number and DES key generation. The RNG also incorporates a continuous random number generation test, which compares current blocks of data to previous blocks to prevent against failure of the random number generator to a constant value.